UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,004	12/07/2001	Bryan Joyner	124143-1000	4989

7590	03/04/2005

Daniel J. Chalker
GARDERE WYNNE SEWELL LLP
Suite 3000
1601 Elm Street
Dallas, TX 75201-4767

EXAMINER
KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 03/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)	
Office Action Summary	10/010,004	JOYNER ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _12/7/2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-87_ is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-87_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _12/7/2001_ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All　b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

Part III. Detailed Action

Drawings

The drawings are objected to because pages 9-10 of the specification refer to element 204

as "decrypted content", whereas fig. 2 refers to the element as "unencrypted content."

Furthermore, in fig. 4a, "flash ROM key storage" has the reference numeral 308, whereas in pg.

14 of the disclosure it is referred to as "key storage 108." Please fix inconsistencies that occur

between the specification and the figures. Corrected drawing sheets in compliance with 37 CFR

1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any

amended replacement drawing sheet should include all of the figures appearing on the immediate

prior version of the sheet, even if only one figure is being amended. The figure or figure number

of an amended drawing should not be labeled as "amended." If a drawing figure is to be

canceled, the appropriate figure must be removed from the replacement sheet, and where

necessary, the remaining figures must be renumbered and appropriate changes made to the brief

description of the several views of the drawings for consistency. Additional replacement sheets

may be necessary to show the renumbering of the remaining figures. Each drawing sheet

submitted after the filing date of an application must be labeled in the top margin as either

"Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not

accepted by the examiner, the applicant will be notified and informed of any required corrective

action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The language should be clear and concise and should not repeat information given in the

title. It should avoid using phrases which can be implied, such as, "The disclosure concerns,"

"The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 12-14, 18-21, 41-43, 47-50, 70-72, and 76-79 are rejected under 35 U.S.C. 112,

second paragraph, as being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention.

As per claims 12-14, 41-43, and 70-72:

These claims recite the limitation "the one or more terms of use" in line 1, where "one or

more terms of use" has not been previously introduced in the parent claim. Thus, there is

insufficient antecedent basis for this limitation in the claim. Applicant may have intended for

these claims to depend on claim 11, which does previously introduce one or more terms of use.

If not, in order to fix this, applicant can adjust the wording by putting it in the same form as is

used for claim 11.

As per claims 18-21, 47-50, and 76-79:

These claims recite the limitation "the communication link" in line 1, where a

"communication link" has not been previously introduced in the parent claim. Thus, there is

insufficient antecedent basis for this limitation in the claim. Applicant may have intended for

these claims to depend on claim 17, which does previously introduce a communication link. If

not, in order to fix this, applicant can adjust the wording by putting it in the same form as is used

for claim 17.

Claim Rejections - 35 USC § 102

I.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

II.   Claims 1-7, 10-27, 30-36, 39-56, 59-65, and 68-85 are rejected under 35 U.S.C. 102(e) as

being fully anticipated by Gruse et al., United States Patent No. 6,389,538.

As per claim 1:

Gruse et al. teach a method of providing encrypted data to a device comprising the steps

of: receiving one or more public keys from the device (col. 16 lines 20-23, col. 35 lines 34-38,

and col. 45 lines 58-64); validating the one or more public keys (col. 45, lines 58-67, where

validating and successfully verifying the signature in turn validates the public key); receiving a

request for the encrypted data from the device (col. 45, lines 44-56); retrieving the encrypted

data and a symmetric key used to encrypt the data (col. 15, lines 37-46 and col. 46, lines 45-57);

encrypting the symmetric key using each of the one or more public keys (col. 18, lines 26-28 and

col. 46, lines 57-64); and sending the one or more encrypted symmetric keys and the encrypted

data to the device (col. 18, lines 38-47 and col. 46, line 61 – col. 47, line 12).

As per claim 2:

Gruse et al. teach the method as recited in claim 1, further comprising the steps of:

receiving data (col. 16, lines 56-65); creating the symmetric key; and encrypting the data using

the symmetric key (col. 18, lines 22-23).

As per claim 3:

Gruse et al teach the method as recited in claim 2, further comprising the step of storing

the symmetric key and the encrypted data (col. 18, lines 38-40).

As per claim 4:

Gruse et al. teach the method as recited in claim 2, wherein the data is compressed (col.

23, lines 3-5).

As per claim 5:

Gruse et al. teach the method as recited in claim 4, wherein the data is compressed using

a Moving Picture Experts Groups ("MPEG") standard (col. 23, lines 3-11).

As per claim 6:

The method as recited in claim 2, further comprising the step of compressing the data

(col. 23, lines 3-5).

As per claim 7:

The method as recited in claim 2, wherein the data is encrypted using a triple Data

Encryption Standard ("3DES") algorithm (col. 15, lines 47-53).

As per claim 10:

Gruse et al. teach the method as recited in claim 1, further comprising the step of

authorizing the request (col. 13, lines 48-55 and col. 45, lines 58-67).

As per claim 11:

Gruse et al. teach the method as recited in claim 1, wherein the encrypted data includes

one or more terms of use (col. 17, lines 59-61).

As per claim 12:

Gruse et al. teach the method, wherein one or more terms of use comprises a view only

once restriction (col. 15, lines 13-18).

As per claim 13:

Gruse et al. teach the method, wherein one or more terms of use comprises a limited time

period to view the data (col. 15, lines 13-18).

As per claim 14:

Gruse et al. teach the method, wherein one or more terms of use comprises a reproduction

restriction (col. 23, lines 19-26).

As per claim 15:

Gruse et al. teach the method as recited in claim 1, wherein the steps of encrypting the

symmetric key using each of the one or more public keys and sending the one or more encrypted

symmetric keys and the encrypted data to the device comprise the steps of: encrypting the

symmetric key and one or more terms of use using each of one or more the public keys; and

sending the one or more encrypted symmetric keys, the one or more encrypted terms of use and

the encrypted data to the device (col. 25, lines 44-47 and col. 40, lines 52-54)

As per claim 16:

Gruse et al. teach the method as recited in claim 1, wherein the step of sending the one or more encrypted symmetric keys and the encrypted data to the device comprises the steps of: creating a file comprising the one or more encrypted symmetric keys and the encrypted data; and sending the file to the device (col. 18, lines 38-47).

As per claim 17:

Gruse et al. teach the method as recited in claim 1, further comprising the step of establishing a communication link with the device (col. 18, lines 41-47).

As per claim 18:

Gruse et al. teach the method as recited in claim 1, wherein the communication link includes a telephone line (col. 9, lines 28-39)[1].

As per claim 19:

Gruse et al. teach the method as recited in claim 1, wherein the communication link includes a wireless connection (col. 9, lines 40-44).

As per claim 20:

Gruse et al. teach the method as recited in claim 1, wherein the communication link includes a satellite connection (col. 9, lines 40-44).

As per claim 21:

---

[1] Although the term "telephone line" is not used, set-top box is mentioned where the definition mentions that it is connected to another communication channel, for example a telephone line. The definition of set-top box as it appears on the Free On-Line Dictionary of Computing is pasted below.

Set-Top Box:
(STB) Any electronic device designed to produce output on a conventional television set (on top of which it nominally sits) and connected to some other communications channels such as telephone, ISDN, optical fibre or cable. The STB usually runs software to allow the user to interact with the programmes shown on the television in some way.

Gruse et al. teach the method as recited in claim 1, wherein the communication link

includes the Internet (col. 9, lines 40-44).

As per claim 22:

Gruse et al. teach the method as recited in claim 17, wherein the step of establishing a

communication link with the device comprises the steps of: establishing a control

communication link with the device; and establishing a data communication link with the device

(col. 14, lines 49-67). Although these steps are not specifically stated, the Internet is used for

communication. The Internet implies the use of TCP/IP, which carries out the steps of

connection establishment and data transfer, thus is inherent.

As per claim 23:

Gruse et al. teach the method as recited in claim 1, wherein the data is an audio/video

transmission (col. 1, lines 58-63).

As per claim 24:

Gruse et al. teach the method as recited in claim 1, wherein the data is a sound recording

(col. 1, lines 58-63).

As per claim 25:

Gruse et al. teach the method as recited in claim 1, wherein the data is a game (col. 1,

lines 58-63).

As per claim 26:

Gruse et al. teach the method as recited in claim 1, wherein the device is an audio/video

playback device (col. 9, lines 49-56). Although the term "playback device" is not used the

functionality of the device disclosed invention is equivalent to that of a playback device.

As per claim 27:

Gruse et al. teach the method as recited in claim 1, wherein the device is a computer (col.

19, lines 40-42).

As per claims 30-36 and 39-56:

These claims are rejected because they are similar in scope to claims 1-7 and 10-27

because they are claiming the computer program on a computer readable medium in the same

way as the rejected method claims above.

As per claims 59-65 and 68-85:

These claims are rejected because they are similar in scope to claims 1-7 and 10-27

because they are claiming the system in the same manner as the rejected method claims above.

Claim Rejections - 35 USC § 103

III.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

IV.   Claims 8, 28-29, 37, 57-58, 66, and 86-87 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Gruse et al., United States Patent No. 6,389,538 as applied to claims 1 (for

claims 28-29), 2 (for claim 8), 30 (for claims 57-58), 31 (for claim 37), 59 (for claims 86-87),

and 60 (for claim 66) above.

As per claim 8:

Gruse et al. substantially teach the method as applied to claim 2 above. Not explicitly

disclosed by Gruse et al. is the method, wherein the data is encrypted using an Advanced

Encryption Standard ("AES") algorithm. However, Gruse et al. teach that any algorithm can be

used for encryption. Therefore, it would have been obvious to a person in the art at the time the

invention was made to modify the method disclosed in Gruse et al. for the data to be encrypted

using AES. This modification would have been obvious because a person having ordinary skill

in the art, at the time the invention was made, would have been motivated to do so since it is

suggested by Gruse et al., col. 15, lines 36-46.

As per claim 28:

Gruse et al. substantially teach the method as applied to claim 1 above. Not explicitly

disclosed by Gruse et al. is the method, wherein the device is a personal data assistant. However,

Gruse et al. teach that the end-user device includes a personal communications service (PCS).

Therefore, it would have been obvious to a person in the art at the time the invention was made

to modify the method disclosed in Gruse et al. for the end-user device to be a personal data

assistant since the term PCS is used to cover a variety of wireless technologies, one of which is a

personal data assistant. This modification would have been obvious because a person having

ordinary skill in the art, at the time the invention was made, would have been motivated to do so

since it is suggested by Gruse et al., col. 9, lines 28-39.

As per claim 29:

Gruse et al. substantially teach the method as applied to claim 1 above. Not explicitly

disclosed by Gruse et al. is the method, wherein the device is a wireless network device.

However, Gruse et al. teach that the end-user device includes a personal communications service

(PCS). Therefore, it would have been obvious to a person in the art at the time the invention was

made to modify the method disclosed in Gruse et al. for the end-user device to be a wireless

network device since the term PCS is used to cover a variety of wireless technologies. This

modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since it is suggested by Gruse

et al., col. 9, lines 28-39.

As per claims 37 and 57-58:

These claims are rejected because they are similar in scope to claims 8 and 28-29 because

they are claiming the computer program on a computer readable medium in the same way as the

rejected method claims above.

As per claims 66 and 86-87:

These claims are rejected because they are similar in scope to claims 8 and 28-29 because

they are claiming the system in the same manner as the rejected method claims above.

V.   Claims 9, 38, and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Gruse et al., United States Patent No. 6,389,538 as applied to claims 1, 30, and 59 above, and

further in view of Schneier, *Applied Cryptography*.

As per claim 9:

Gruse et al. substantially teach the method as recited in claim 1. Not explicitly disclosed

by Gruse et al. is the method, wherein the data is encrypted using a symmetric linear feedback

shift register ("LFSR") sequence. However, Schneier teaches that a linear feedback shift register is the simplest kind of feedback shift register to implement. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Gruse et al. to encrypt the data by using a symmetric linear feedback shift register. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Schneier on pg. 373, par. 2-3.

As per claim 38:

These claims are rejected because it is similar in scope to claim 9 because it is claiming the computer program on a computer readable medium in the same way as the rejected method claim above.

As per claim 67:

These claims are rejected because it is similar in scope to claims 28-29 because it is claiming the system in the same manner as the rejected method claim above.

*References Cited, Not Used

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. U.S. Patent No. 5,646,999
2. U.S. Patent No. 6,438,235
3. U.S. Patent No. 6,499,106

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.
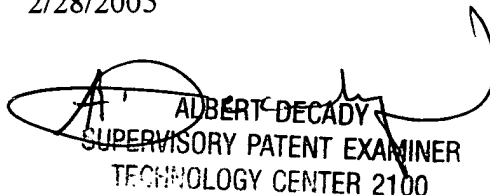
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2133
2/28/2005

NK

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100